STATEMENT OF

MARK A. FORMAN

ADMINISTRATOR, OFFICE OF ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY

OFFICE OF MANAGEMENT AND BUDGET

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

May 8, 2003

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to discuss how the Administration is working to improve Homeland Security through improved Federal IT management, including improved coordination and elimination of redundant IT investments, E-Government efforts, and use of enterprise architectures (EA).

Mr. Chairman, making organizations share information is like trying to glue together thousands of puzzle pieces. If the pieces are put together correctly, you get a pretty picture. If you just apply the glue without an orderly approach to building the puzzle, you could end up with something quite messy that doesn't look at all like the real picture. One of the challenges for the Department of Homeland Security is to get better results from available information. The need is not about connecting dozens of overlapping databases, but bringing order and structure to homeland security efforts by eliminating redundant systems, developing information sharing solutions, and making it all work together. As laid-out in the President's Management Agenda initiatives for E-Government and Information Technology, we believe we can obtain measurably better results in mission critical areas by simplifying and unifying organizations, processes, and information technology.

Bringing together twenty-two previously separate agencies and offices under one Department requires more architecting than merely gluing together all of their IT. As recognized by the Chairman's invitation letter, interoperability needed for Homeland Security must extend beyond information sharing. The Administration uses best practices in e-business and IT management to assist in

setting priorities and defining an action plan. Last June, the President's proposal for the Department of Homeland Security highlighted the use of EA techniques to improve both sharing and use of information. The President stated: "Development of a single enterprise architecture for the department would result in elimination of the sub-optimized, duplicative, and poorly coordinated systems <and processes> that are prevalent in government today. There would be rational prioritization of projects necessary to fund homeland security missions based on an overall assessment of requirements rather than a tendency to fund all good ideas beneficial to a separate unit's individual needs even if similar systems are already in place elsewhere."

Indeed, the Administration believes good EA analysis is needed to build integrated business processes and organizations. To be an effective tool, the EA has to reflect organizational decisions made by agency leadership and be owned and used by agency leadership in making resource decisions. Agency decisions must reflect the key elements of the President's Management Agenda, optimizing performance while trading-off human capital, IT and other resources. As identified in the National Strategy for Homeland Security, there are two primary measures of performance to be used in the federal homeland security IT initiatives: (1) improving response time – the time to detect and respond to potential threats; and (2) improving decision-making – making the right decisions at the right time. All homeland security IT investments must accelerate our response times and improve our decision making, and doing so requires significant changes in long-standing organizations, processes, information flows, and IT investments.

Mr. Chairman, as we have discussed before, there are a number of issues that must be addressed to get value from the Department of Homeland Security's IT investments. At a minimum we have identified agency culture, public trust, resources, stakeholder resistance, and lack of both a Federal EA as well as individual agency EAs as all potential barriers to be overcome through effective management of IT resources.

## Improving Agency use of Information and IT

OMB provides guidance and works with Federal agencies to ensure that the Federal government applies best

practices in IT management. Through traditional budget and management processes, we hold all agencies accountable for meeting the statutory and policy requirements defined below. Four of the key components are:

**1. Enterprise Architectures.**

An EA describes how an organization performs its work using people, business processes, data, and technology. By aligning organizations, business processes, information flows, and technology, EA tools are used to build a blueprint for improving efficiency and effectiveness of an organization. OMB operates the Federal Enterprise Architecture Program Management Office, created last year, to work with Federal agencies in developing a government-wide EA. The FEA is a business-focused framework developed for OMB, federal agencies and Congress to use in improving the performance of government.

The FEA framework addresses five important areas of enterprise architecture, tying together the business, performance, service, technology, and data layers.

Through the *Business Reference Model (BRM)* we identify the Federal government's business operations and the agencies that perform them. This information helps to prevent potentially redundant IT investments in the Federal government's business lines, ultimately resulting in cost savings and productivity growth. *Version 2.0* of the model will be released later this month for all agencies to use in the FY 2005 budget formulation process.

The *Performance Reference Model (PRM)* is a framework that agencies will use to link IT investments to mission performance measures. The model allows OMB and agencies to identify common measurements and set baselines and targets. OMB has released the Working Draft PRM for Federal agency review and comment.

The *Service Component Reference Model (SRM)* provides the foundation for the re-use and sharing of IT across Federal agencies, and potentially across Federal, state and local governments.

The *Technical Reference Model (TRM)* outlines the technology elements that support the service components. The TRM will be used to facilitate both interoperability and the transition to e-government by reducing the complexity and isolated nature of many Federal systems, encourage the sharing of infrastructures across agencies, and reduce IT costs.

The *Data and Information Reference Model (DRM)* will provide a consistent framework to characterize and describe the data that supports Federal business lines. This will promote interoperability, as well as the horizontal and vertical sharing of information. OMB is working collaboratively with a small group of interested Federal agencies to define and validate the model, and a draft will be released soon for agency review and comment soon.

In addition, OMB and the Federal CIO Council are developing the Federal Enterprise Architecture Management System (FEAMS). FEAMS is a web-based tool to enhance FEA analysis and maintenance, and agencies' capital planning and investment control efforts. In addition to storing the FEA reference models, FEAMS will include general information on agencies' IT initiatives.

We are actively working with the Department to ensure that they develop a comprehensive EA that optimizes the existing investments inherited from the legacy agencies. This includes identifying redundant investments, developing new solutions, and linking together existing systems.

## 2. Managing and Budgeting IT Investments

OMB IT management (OMB Circular A-130) and budget (OMB Circular A-11) guidance addresses information sharing at a system by system basis through the agency budget request or business case for each IT investment. We are working with all agencies to ensure that they appropriately leverage and consolidate their IT investments (infrastructure, business management systems, and mission-related IT) within and across their directorates.

In particular, the merging of twenty-two previously separate agencies has resulted in DHS inheriting a number of redundant and overlapping IT systems and processes. The Director of OMB, in Memoranda M-02-12 and M-02-13, issued guidance under the Clinger-Cohen Act on consolidating and integrating IT investments across agencies performing homeland security missions. Through the FY 2005 budget process, OMB will work with the Department to eliminate redundant and non-integrated operations, systems, and processes for business and mission areas. Through consolidated business cases, the relevant systems for consolidation are listed, plans for migration and elimination are reported, and an integrated business process identified. Additionally, each business case must identify specific performance measures – how are we

advancing our homeland security goals through the requested investment, what performance improvement will we achieve? IT investments that support homeland security missions must be appropriately integrated in order to leverage technology for mission effectiveness while preventing redundant investments and wasted resources.

Additionally, I would like to highlight recent guidance issued by the Director of OMB to Federal agencies on planning for the President's FY 2005 Budget Request. To further strengthen IT and E-Government efforts, Federal agencies were instructed to ensure that IT budget information is fully integrated with each FY 2005 budget request justification, demonstrate solid business cases for IT projects, and identify all IT investments within their budget request. DHS will be held to this standard like any other Department. We are working with them to strengthen the use of IT in homeland security efforts.

**3. E-Government Initiatives.**

As you know, the Administration has been aggressively working over the last year and a half in the development and implementation of twenty-four government-wide Presidential E-Government initiatives. Implementation of the President's E-Government initiatives related to homeland security will overcome information sharing difficulties between Federal, state, and local organizations and first responders. In addition, many of the other Presidential E-Government Initiatives provide solutions that must be adopted by all departments. These initiatives include E-Authentication as well as a new initiative on public health information.

The goal of E-Authentication is to minimize the burden on businesses, the public and government when obtaining services online by providing a secure infrastructure for online transactions, eliminating the need for separate processes for the verification of identity and electronic signatures. However, a large portion of E-Authentication involves policy work. As the Federal government modernizes internal processes to reduce costs for agency administration and moves to cross agency applications that are available to all Federal employees, common solutions for authentication are needed. The first step of which is the development of policy to implement standardized

identity credentials across the Federal government, which all Departments will implement.

Public Health Monitoring involves activities associated with monitoring the public health and tracking the spread of disease. For FY 2003 and FY 2004 requests for projects valued at $ 267 M and $ 296 M were received by OMB. Requesting agencies included HHS and VA. Areas of potential overlap included: health information surveillance, emergency response and addressing "early warning" and alerts, decision support and case management functionality.

Two of the President's initiatives, Project Safecom, and Disaster Management, directly support and promote improving information sharing between Federal, state, and local first responders. The goal of Project Safecom is to provide interoperable wireless options for Federal, state and local public safety organizations and ensure they can communicate and share information as they respond to emergency incidents. Disaster Management provides Federal, state, and local emergency managers online access to disaster management-related information, planning and response tools. Both of these initiatives strongly support "vertical" (i.e. intergovernmental) integration necessary to meet homeland security goals.

Because these two initiatives clearly support homeland security missions and activities within the Department of Homeland Security, OMB placed it as the managing partner for the initiatives. As managing partner, DHS is responsible for ensuring the accuracy of the business cases for these initiatives, submitting the business cases, and ensuring the management of the projects to achieve the cost, schedule and performance goals for the implementation and operations phases.

Additionally, as part of the recent OMB guidance to agencies on FY 2005 budget planning, and to ensure that E-Government initiatives are appropriately supported, OMB will provide each agency's funding or other resource requirements as outlined in the FY 2004 President's Budget, for participation in the Presidential E-Gov Projects, consistent with requirements under the E-Government Act of 2002.

**4. President's Management Agenda**

OMB monitors progress on all of these items on a regular basis through the President's Management Agenda Scorecard under the Expanding E-Government Score. Inability to achieve the core criteria under the E-Government Scorecard will prevent an agency from "getting to green". As true information sharing is dependent on a number of factors as I have discussed -- development and implementation of an effective EA, appropriate planning and budgeting for IT investments, and successful achievement of E-Government initiatives, -- failure to overcome barriers will directly impact an agency's E-Government Score. Because the Department of Homeland Security is new, it's status is scored as "red." We are actively working with them to achieve real progress in the next several months.

Conclusion

The Administration will continue to work collaboratively across Federal agencies, with Congress, State and local governments, and the private sector to strengthen information sharing in support of homeland security efforts. Achieving true homeland security will require IT investments that both guarantee real-time information sharing, and successfully improve response time and decision-making. To meet these goals and assist in overcoming information sharing barriers, we require wise IT investments that support homeland security missions, enhance productivity, ultimately facilitating information sharing while ensuring security and privacy.

While we recognize that the Department is currently grappling with cultural legacies of twenty-two component agencies, we fully expect that DHS leadership will continue to build an integrated and interoperable structure, resulting in a business driven EA that reflects the President's vision of eliminating "sub-optimitized, duplicative, and poorly coordinated systems." OMB will continue to work with DHS leadership, including the Chief Information Officer to ensure that their EA efforts, their integration of business process, and consolidation and elimination of redundant IT investments remains a top priority and is addressed in a timely manner. We will assess their efforts on a regular basis and use the President's Management Agenda Scorecard to monitor their progress against detailed milestones.